DATE(S) ISSUED:
3/9/2010

SUBJECT:
Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (MS10-017)

OVERVIEW:
Multiple vulnerabilities have been identified in Microsoft Office Excel, Microsoft's spreadsheet application. These vulnerabilities could allow remote code execution if a user opens a specially crafted Excel document. The document may be received as an email attachment, or downloaded via the Web. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- · Microsoft Excel 2002

- · Microsoft Excel 2003

- · Microsoft Excel 2007

- · Microsoft Excel Viewer

- · Microsoft Office XP

- · Microsoft Office 2003

- · 2007 Microsoft Office System

·   Microsoft Office for Mac

·   Microsoft Office 2004 for Mac

·   Microsoft Office 2008 for Mac

·   Open XML File Format Converter for Mac

·   Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats

·   Microsoft Office SharePoint Server 2007

RISK:

Government:

·   Large and medium government entities: High

·   Small government entities: High

Businesses:

·   Large and medium business entities: High

·   Small business entities: High

Home users: High

DESCRIPTION:
Seven vulnerabilities have been identified in Microsoft Office Excel that could allow an attacker to take complete control of an affected system. These vulnerabilities can be triggered by opening a specially crafted Excel document (.XLS) and can be exploited via email or through the Web. In the email based scenario, the user would have to open the specially crafted Excel document as an email attachment. In the Web based scenario, a user would have to open the specially crafted Excel document that is hosted on a

website. When the user opens the Excel document the attacker's supplied code runs. Microsoft Office Excel 2002 and later versions have a built-in feature that prompts a user to Open, Save, or Cancel before opening a document.

The seven vulnerabilities are as follows:

Microsoft Office Excel Record Memory Corruption Vulnerability
This vulnerability is caused by a memory corruption error when processing malformed "EntExU2" records, which could be exploited by a user opening a specially crafted Excel document.

Microsoft Office Excel Sheet Object Type Confusion Vulnerability
This vulnerability is caused by a memory corruption error when processing malformed "BRAI" BIFF records, which could be exploited by a user opening a specially crafted Excel document.

Microsoft Office Excel MDXTUPLE Record Heap Overflow Vulnerability
This vulnerability is caused by a memory corruption error when processing malformed data related to "MDXTuple" and "ContinueFRT12" records, which could be exploited by a user opening a specially crafted Excel document.

Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability
This vulnerability is caused by a memory corruption error when processing malformed data related to "MDXSet" and "ContinueFRT12" records, which could be exploited by a user opening a specially crafted Excel document.

Microsoft Office Excel FNGROUPNAME Record Uninitialized Memory Vulnerability
This vulnerability is caused by a memory corruption error when processing malformed data related to "FnGroupName", "BuiltInFnGroupCount" and "FnGrp12" records, which could be exploited by a user opening a specially crafted Excel document.

Microsoft Office Excel XLSX File Parsing Code Execution Vulnerability
This vulnerability is caused due to an uninitialized pointer when processing malformed data, which could be exploited by a user opening a specially crafted Excel document.

Microsoft Office Excel DbOrParamQry Record Parsing Vulnerability
This vulnerability is caused by a memory corruption error when processing malformed "DbOrParamQry" records, which could be exploited by a user opening a specially crafted Excel document.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated

with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without   administrative privileges) to diminish the effects of a successful   attack.
- Remind users not to open email attachments from unknown or un-trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Consider using the Microsoft Office Isolated Conversion   Environment (MOICE - http://support.microsoft.com/kb/935865) to   mitigate some of the vulnerabilities identified in this advisory.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-017.mspx

Vupen:
http://www.vupen.com/english/advisories/2010/0566

Security Focus:
http://www.securityfocus.com/bid/38555
http://www.securityfocus.com/bid/38554
http://www.securityfocus.com/bid/38553
http://www.securityfocus.com/bid/38552
http://www.securityfocus.com/bid/38551
http://www.securityfocus.com/bid/38550
http://www.securityfocus.com/bid/38547

Secunia:
http://secunia.com/advisories/38805/